Blackfen School's Acceptable User Policy for School's ICT Network, School email and Internet

Date: Oct 2016 **LT lead: Assistant Headteacher Curriculum**

Rationale

Blackfen School for Girls believes that the appropriate use of ICT & new technologies improves students learning and the teaching across the curriculum to good or outstanding. The policy outlines the practice expected of all users in order to maintain and develop our provision. It sets out the legal aspects and identifies the responsibilities of all users of the resources

This policy is part of the developing of e-safety at Blackfen and the embedding of the following principles in the practices of all staff, students and stakeholders

- Keep all personal information private
- Consider the long term implications of any content posted on-line
- Do not upload or post inappropriate, offensive or illegal content to their own or other online spaces
- Read and adhere to any website's terms and conditions of use, including those around age restrictions

Outcomes

The school provides a safe & reliable working environment which enables all users to benefit from the technology in place

Legal Procedures

All users must obey the applicable laws relating to the use of IT services, Freedom of Information, Data protection and respect copyright as set out in Appendix 3 Legal procedures

Use of the School Network, School Email and Internet (in school or out of School) all users must:

- Read the School bulletin & check their school email daily (Staff only)
- Follow the guidance in Appendix 1 when using the School email systems
- Be polite. Never send or encourage others to send abusive messages. Always use appropriate language. Remember that you are a representative of the school, and others can view what you say.
- Always respect the rights and beliefs of others, and remember that humour and satire can often be misinterpreted.
- Never reveal personal information to anyone, especially a home address, a personal telephone, a personal login and/or password to the School Network, website, social networking site etc
- Contact CTS immediately (Staff can ring Extension 3115) if you think someone has obtained any of your personal information
- Never disrupt use of the services by others. This includes trying to 'hack' any system to get around any security measures put in place to protect it & yourself
- NOT attempt to plug personal laptops or any other personal devices into the network
- Be aware that the school network & email and Internet use is monitored by staff and if it is found that they are being abused, then the facilities may be withdrawn without notice.

Use of Hardware, all users must

- Never attempt to move, disconnect or in any other way, tamper with any IT equipment and never attempt to rectify faults in equipment. All faults should be reported to CTS in the usual ways.
- Never leave a PC unattended to which they are logged into. Always save your work and log out. The School reserves the right to log out any user and are not responsible for the loss of any unsaved work.
- Only use external hard drives for storage or back-up – Always save work into your user area.
- log out of a shared computer (e.g. in the Library) for someone requiring it for study or other legitimate use if they are using for recreational purposes

Use of Internet based Social Media (e.g. Facebook, Twitter, Snapchat, YouTube, PinInterest, Instagram, WhatsApp etc)

Staff

- must not have students or their parent/carer(s) as their friend, contact or similar and must not attempt to contact students or their parent /carer(s) via social media
- must block or delete parents and students attempting to follow them via social media
- should not publish anything on social media that they would not want their employer or students to see.
- must not use social media to discuss school matters of a confidential matter or that are in anyway critical of the School.
- must not put anything on these sites that could damage, yours, the School's or anybody connected to the School's reputation. (Photographs etc;)
- must never use their own cameras or phone to record, photograph or film children in school.
- finding their image or a video clip from school on the internet should take the following action: (1) Contact the site directly to have the item removed; (2) Inform the link LT to report the incident

Staff NB - if the AUP use of social media is not followed, as outlined above, an investigation may be carried out and this could ultimately lead to disciplinary action**.** In the case of governors, it could lead to suspension, as it may damage the reputation of the School's Governing Body.

Please be aware that access to most social media sites via the School network or Internet connection are blocked. Members of LT, Room 2 & other designated staff have access to these sites to check content and investigate incidents of misuse.

Staff should regularly check their security settings on social media. These security settings are often changed by the provider and so staff should check these regularly. It is recommended that security settings are set to the highest level, e.g. 'Friends only' on Facebook, so that private and personal information, photographs etc cannot be seen publically by those other than your 'friends', followers or similar.

Students

- Should not publish anything on social networking sites that identifies themselves as a Blackfen student
- Should not publish anything on social networking sites that they would not want their parent/carer or other responsible adult to see

- Should not publish anything on social media about a Blackfen student or their family and friends, including their image without gaining their permission first
- Should never publish anything on social media about anyone employed by Blacken School for Girls, including their image.
- Need to be aware that bullying another Blackfen student using the Internet, social networking sites, the School network, Fronter, School e-mail etc is still bullying and will be treated as such by the School. Students can expect to be sanctioned as set out in the Behaviour Charter, whether the incidents have been posted in School or out of School

- caught viewing or sharing inappropriate material, including that of another student or persons employed by the School, on a computer or on their mobile device via social media or otherwise, will receive a serious sanction. The School has a robust filter for the internet and a system for monitoring computer usage, However, out of School and particularly on mobile phones connected to the mobile networks, there is often no supervision, monitoring or filtering.

Students NB - if the AUP is not followed, as outlined above, there will be an investigation carried out and in most cases this will result in at least a serious sanction, exclusion or the School reporting a student to the Police. The School has a robust filter for the internet and a system for monitoring computer usage, However, out of School and particularly on mobile phones connected to the mobile networks, there is often no supervision, monitoring or filtering. It is therefore a student's responsibility to adhere to this guidance or face the consequences of their actions

Key roles

AHT (Curriculum) & CTS: to liaise with staff to ensure implementation of procedures; to ensure that the AUP Policy is published to staff, students and parents and is reviewed according to schedule.
FLs: to ensure implementation of AUP procedures by their staff and the students whilst in their Faculty lessons
Tutors & SSOs: to ensure implementation of AUP procedures by the students whilst in Community time and out of lessons
Teachers: to be aware of and to follow school AUP policy and to ensure students adhere to this at all times
Students: to be aware of and follow school AUP policy at all times

Related documents - Curriculum Policy, Behaviour for Learning Policy, Anti-Bullying Policy, Safeguarding Policy, Code of Conduct, Health & Safety Policy and Behaviour Charter 2016-17
Review cycle: Annual Next review: Oct 2017

Appendix 1 - Email

Under the Freedom of Information Act 2000, your School email is not private. Therefore, any email sent or received from/to a School account is School property and can be used and disclosed to third parties if appropriate. Please note that writing an email about someone is treated the same as putting it on paper in the eyes of the Law.

Do not send email to people you do not know, unless you have a good reason and always re-read a message before sending

Staff should only delete emails that they do not need to retain. If an email contains a discussion about a student or a member of staff, it should be retained or archived

Students should only access their Email in their free time in School unless directed by a teacher to do so in lesson

If Staff or a student receives an Email which upsets them in some way e.g. it is abusive or harassing, forward it to askit@blackfen.bexley.sch.uk and contact your line manager

Appendix 2 – Teacher Standards Sept 2012

In the Teacher Standards that came into force in September 2012, under Personal and Professional Conduct 'A teacher is expected to demonstrate consistently high standards of personal and professional conduct.'

If a member of staff found not to be adhering to the AUP Policy as described above they may find this being taken into consideration as part of their Appraisal process and could result in a member of staff facing disciplinary action.

Appendix 3 – Legal Procedures
All students, staff and stakeholders MUST

- Obey the applicable laws relating to the use of IT services, notably Complying with the Computer Misuse Act 1990 and the Criminal Justice Act 1994 amendment to the Obscene Publications Act under which it is a criminal offence to; create, store, download or transmit obscene material, hack or the deliberately introduce a virus.
- Adhere to the applicable laws relating to public authorities, notably the Freedom of Information Act 2000
- Respect the copyright of all materials and software that are made available by the school and comply with the requirements of the Data Protection Act (19880. E.g. staff should not be showing a film, a TV programme, play a downloaded song on DVD or CD unless it is for educational purposes
- not store electronic copies of copyrighted material like films or songs anywhere on the school IT network
- Make themselves aware of the Prevent Strategy June 2011 and subsequent updates, and its application to the use of School ICT Network, School email and use of the Internet
- Make themselves aware of the School's latest Safeguarding Policy and its application to the use of the School ICT Network, School email and use of the Internet